UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,367	03/15/2001	Edward J. Hogan	AP33088-070457.0985	5526

7590 12/09/2008

BAKER BOTTS L.L.P.
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112-0228

EXAMINER	
FISCHER, ANDREW J	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/809,367
Filing Date: March 15, 2001
Appellant(s): HOGAN ET AL.

Robert C. Scheinfeld, Reg. No. 31,300
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6 October 2006 appealing from the Office action mailed 4 October 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is not correct. This Examiner's answer contains a new grounds of rejection.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,163,771	WALKER et al.	12-2000
6,636,833	FLITCROFT et al.	10-2003
6,018,717	LEE et al.	1-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Response to Amendments/Arguments

In response to Applicant's arguments, the 112 second paragraph rejection to claims 1-10 is withdrawn. However, the other rejections are maintained by the Examiner.

Applicant's Specification does not support a "second payment account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser". To the contrary, Applicant merely states that "if unauthorized persons were to ascertain any pseudo account numbers, they would be unable to make fraudulent transactions using them" a clear nod to Applicant's use of encryption for authenticating transactions (page 3, paragraph [0008]). Nor would this citing support the limitation of a "second payment account

number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser". A system that utilizes a pseudo payment number for transactions protects the master payment number because the main number is not revealed to a merchant. Therefore, to one of ordinary skill if a second or pseudo number is compromised one of ordinary skill would create a new pseudo number (similar to the single use embodiment of Flitcroft et al. where after a card number is used it is invalidated and the user moves on to a new pseudo number- column 13, lines 38-57; column 23, lines 28-38).

Regarding the prior art, a "second payment account number being reusable by the purchaser for as long as the first payment account number is usable by the purchaser" is clearly taught by the system of Flitcroft et al.. Specifically, Flitcroft et al. teach pseudo numbers whose only restrictions are limitations directed to a specific location (column 8, lines 1-10 and 24-30), a specific merchant (column 16, lines 57-59), or a specific purpose (column 8, lines 1-10). Hence, a number can be reused, for example, as long as a consumer is making purchases over the internet (column 8, lines 7-10). However, if the master card number is invalidated then the pseudo number cannot be authorized (figure 7, item 714; column 25, lines 12-33). More specifically, Flitcroft states that if the master number is closed or delinquent then the pseudo number is no longer accessible (column 24, lines 30-37).

Claim Rejections - 35 USC § 112

Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1 recites a second payment number being reusable, "by the purchaser for as long as the first payment account is usable by the purchaser". Claim 4 contains a similar recitation. However, this limitation is not supported by the Specification. While Applicant discloses the one-to-one relationship that exists between a real and pseudo card numbers (Specification, figures 3a-b; paragraph [0008]), to one of ordinary skill if it is determined that the pseudo-number is no longer trusted or it has been compromised, a user can still use the first number and a new pseudo-number would be calculated, thus leaving the old pseudo number obsolete.

Claims 2 and 3, and 5-10 are also rejected as they depend from claims 1 and 4, respectively.

Claim Rejections - 35 USC § 103

Claims 1-7, 9, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al., U.S. Patent No. 6,163,771 in view of Flitcroft et al., U.S. Patent No. 6,636,833.

As per claims 1-7, 9, and 10, Walker et al. teach a method for conducting a secure transaction by providing users with a list of proxy credit card numbers (column 11, lines 20-25) comprising:

- assigning to a purchaser a first payment account number (real credit card number) having a status that changes over time, providing a second payment account number (pseudo credit card number) and having an encryption key assigned thereto (figures 7, 8 and 13; column 7, lines 20-26)
- requesting authorization for payment of said transaction with the second (pseudo) number and not the first (real), identifying said purchaser's first payment number in response to the authorization request and responding to the authorization request based upon the status of the first number, based on a credit balance that changes over time (figures 3B, 9A-B, and 10-11B; column 7, lines 20-26)
- a response to the authorization request is based on cryptographic code based on said encryption key (figures 6 and 9A-B; column 7, lines 28-51)

- providing a purchaser with a secure payment application which includes a cryptographic key that is unique to the first account number and a second or pseudo account number of the same length as the first (figures 6 and 7; column 6, lines 30-53; column/line 7/27-8/36)
- providing a purchaser with merchant data and generating a message authentication code as a function of merchant data and said cryptographic key and providing a merchant with the code and the pseudo account number (figure 3B; column 6, lines 15-28; column 9, lines 30-36)
- cryptographically processing the pseudo account number to produce the first account number (column/line 8/1-9/9)
- differentiating the pseudo number from the first number by special identifier within the pseudo account number, and by data within a transaction record (figures 7, 8 and 13; column 7, lines 37-51; column 8, lines 9-36)
- cryptographic key is a secret key (abstract)

Walker et al. do not specifically recite verifying that merchant data is correct. However, it would have been at least obvious to one of ordinary skill for a user or

merchant to verify the amount to ensure that the user is being billed properly, and for the user, merchant or credit card issuer to verify the correctness of the merchant ID in order to prevent transaction cancellation based on an incorrect merchant ID. Regarding DES and DESX, Walker et al. implement their system using cryptographic algorithms (column 2, lines 30-34; column 7,lines 3-8). Hence, it would have been obvious to one of ordinary skill to encrypt the pseudo account number using RSA, DES or its variants such as DSA or DESX. Walker et al. do not explicitly recite re-usable pseudo account numbers. Flicroft et al. teach a credit card system for providing users with limited-use card numbers (e.g. single use, reusable) (abstract; column 6, lines 52-64). Specifically, teach a system for creating an encrypted list proxy or second card number from a first (e.g. via mapping, no discernable link for obtaining the first number from the proxy, additional card numbers cannot be predicted from those proxy numbers previously issued) (column 10, lines 8-11; column 11, lines 10-14; column/line 12/10-13/15; column/line 19/65-22/57). Flicroft et al. also teach limiting pseudo-card use based on a prescribed threshold (column 6, lines 52-64). For example, Flitcroft et al. teach pseudo cards that are valid as long as the sum of the transaction in which the cards are used does not accumulate to a limit (column 7, lines 55-64). Further, Flicroft et al. teach pseudo cards that are limited only by

geographic location and purpose (column 8, lines 1-10 and 24-30), hence, Flicroft et al. teach second or pseudo cards that are reusable as long as the real or first number is reusable. Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Walker et al. ('771, figure 13) and Flitcroft et al. in order to create a more flexible system by allowing users to use proxy card numbers for multiple transactions ('833; column 6, lines 52-64) and obtain additional lists of numbers ('771, figure 13, column 11, lines 20-25; '8.33, column 18, lines 25-44; column 19, lines 10-15)

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al., U.S. Patent No. 6,163,771 and Flitcroft et al., U.S. Patent No. 6,636,833 as applied to 4, and in further view of Lee et al., U.S. Patent No. 6,018,717.

As per claim 8, Walker et al. teach a message authentication code that comprises a digital signature generated by a secure payment application (column 8, lines 9-36). However, Walker et al. do not specifically recite public key certificates. Lee et al. teach a method for performing secure transactions using card unique certificates that are associated with a public key of a private/public key pair (column/line 11/15-12/18). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Walker et al. and Lee et al. in order to uniquely associate a transaction message with a user ('717, column/line

10/38-11/13) and to, in the event the private key ('771, abstract) is obtained by a malicious user, to provide protection against fraud by using different keys to encrypt and decrypt a transaction message ('717, column/line 10/38-11/13).

NEW GROUNDS OF REJECTION

Claim Rejections - 35 USC § 101

Claims 1-10 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent[1] and recent Federal Circuit decisions, a §101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. See *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008) (en banc).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps.

To meet prong (1), the method step should positively recite the other statutory class (the thing or product) to which it is tied. This may be accomplished by having the claim positively recite the machine that accomplishes the method steps. Alternatively or to meet prong (2), the method step should positively recite identifying the material that is being changed to a different state or positively recite the subject matter that is being transformed.

---

[1] See also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876).

In this particular case, the claim(s) fail prong (1) because the method steps are not tied to a machine and can be performed without the use of a particular machine. In this case, the method steps appear to be purely mental processes. Additionally, the claim(s) fail prong (2) because the method steps do not transform the underlying subject matter to a different state or thing.

(10) Response to Argument

Mapping of the prior art of Walker et al. and Flitcroft et al. to the broadest claim.

Claim 1	Walker et al. - US Patent No. 6,163,771, Flitcroft et al.- U.S. Patent No. 6,636,833
Assigning to said purchaser a first payment account number having status which changes over time	"Cardholder Account Number" '771, figure 7

	"... to generate a single use financial account identifier" ('771, abstract) "Display encrypted single-use credit card number" ('771, figure 8, item 806)
Providing a second payment account number associated with said first payment account number, said second payment account number being reusable by the purchaser for as long as the first payment account number **is usable by the purchaser, and not being a transaction number and having an encryption key assigned thereto**	"The term **"limited-use"** credit card number is used to encompass **at least both** the embodiment in which the credit card is designated for a **single use**, and the embodiment in which the credit card is designated for multiple uses... **do not exceed a prescribed threshold or thresholds**, such as a total single charge, total charges over a limited time period, total charge in a single transaction, etc.... limited use credit card **can be limited to a single use for a preset amount**" ('833, column 6, lines 52-64)
Requesting authorization for payment of said transaction with said second payment account number and not said first account number	'771, Figures 3A and 9A, item 901 "Receive Encrypted credit card number"

Identifying said purchaser's first payment account number in response to said authorization request; and	'771 Figure 9A, items 901, "Receive Encrypted credit card number", 902 "extract... account number from encrypted credit card number" 903, "Look up account number..." 904 "Does number represent a valid account"
Responding to said authorization request based upon said status of said first payment account number at the time of the transaction	'771, figure 9A items 905 and 907 "abort transaction", item 928 "generate authorization code"

112 First paragraph

Claims 1-3 and 4-10 recite a second payment account number or pseudo account number "reusable by the purchaser for as long as the first payment account number is usable by the purchaser". According to the MPEP (2164.08),

> The record must be clear so that the public will have notice as to the patentee's scope of protection when the patent issues. If a reasonable interpretation of the claim is broader than the description in the specification, it is necessary for the examiner to make sure the full scope of the claim is enabled .

Appellant's method is directed to a method of securing transactions within the credit card art (Specification, page 3, paragraph [0007]). One of ordinary skill in this art understands that when a card number is comprised the number is invalidated in order to protect the card owner from future misuse by a thief or hacker, for example. Therefore, Appellant's statement is false because given the above scenario, while the second or pseudo number is invalidated the first account, if not compromised, will remain in use (note: if a debit card is stolen a new debit card is issued but the number to the bank account remains unchanged).

112 second paragraph

Claim 1 recites "requesting authorization for payment of said transaction with said second payment account number and not said first payment account number". According to Appellant's Specification however, both the pseudo and real account numbers are used to verify the transaction (Specification, figures 4a and 4b (item "D_1" where the "Translation Key" is applied to the "Pseudo Acct#" to reveal the "Real Acct#")). In other words, the Examiner is interpreting the sending of the second or pseudo account number to a merchant as a *request* to include the first account number in the authorization for payment process as the first account number is what ultimately authorizes the transaction and not the second or pseudo account number. The Examiner readily admits that *only* the second or pseudo account number is sent by the cardholder to the merchant (Specification, figures 4a and 4b; paragraph [0027], page 19), however, this is not what Applicant is claiming.

103 rejection

Claims 1 and 8

Appellant is of the opinion that the prior art does not teach "a second payment account number or pseudo account number that is both reusable and that ***may*** be used for as long as the first payment account is usable" (emphasis added) (Appeal Brief, page 13, "In short..."). Initially, the Examiner would like to point out that this is not what is claimed. Claim 1 specifically recites "... said second payment account number being reusable by the purchaser for as long as the first payment account number is usable by

the purchaser..." and the Examiner contends that this is clearly obvious in light of the prior art. Walker et al. teach generating a second or pseudo account number, using said number in a purchase transaction, using the second or pseudo account number to retrieve a first account number and using the first account number to authorize the transaction ('771, abstract; figure 3a). However, Walker et al. do not teach reusable account numbers, in fact Walker et al. teaches "single use" second or pseudo account numbers. So the question is did reusable second or pseudo account numbers exist prior to Appellant method and if so, what it have been obvious to introduce reusable second or pseudo account numbers to the teaching of Walker et al.? Flitcroft et al. teach both single use and limited use second or pseudo account numbers ('833, abstract; column 6, lines 32-64). Hence, one of ordinary skill at least is provided with a teaching of second or pseudo account number than can be single use or reusable. Appellant asserts that "limited use" is not reusable. The Examiner respectfully disagrees. Flitcroft et al. clearly teach second or pseudo account numbers that can be re-used, for example, as long as the total number of charges does not exceed a threshold within a prescribed time period ('833, column 6, lines 55-60). Flitcroft et al. also discloses second or pseudo account numbers assigned to a family or employees of a company where each of the second or pseudo numbers direct back to a master or first account number ('833, column 6, lines 45-52). Therefore, one of ordinary skill would instantly see the benefit of adding reusable second or pseudo account numbers to the system of

Walker et al. as it allows for a more flexible system; where a primary first account holder such as a parent or company CEO can customize the type of second or pseudo account number method to meet a particular need or application such as a child using a single use number to purchase a gift at the mall, or an employee using a reusable account number while on a corporate assignment.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Joshua Murdough

Vincent Millin
Appeals Practice Specialist

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

WYNN W. COGGINS
TECHNOLOGY CENTER DIRECTOR